UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/487,049	01/19/2000	Mohammad Reza Shafiee	Bell Atlantic-17	2681

32127 7590 03/24/2004

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
HAYES, JOHN W	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 21

Application Number: 09/487,049
Filing Date: January 19, 2000
Appellant(s): SHAFIEE ET AL.

Mr. Joel Wall
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 30 January 2004.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is incorrect. Appellant states that all amendments have been entered and that no amendments were filed subsequent to the final Office Action mailed on 23 June 2003. Examiner notes that a Request for Reconsideration (Paper No. 14) was filed after the final Office Action. Although this paper did not attempt to amend the claims, this paper was not entered and was addressed by the examiner in the Advisory Action mailed 06 November 2003.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

The appellant's statement in the brief that certain claims do not stand or fall together is not agreed with for the following reasons. Appellant has not provided separate arguments with respect to Group VIII and has not provided separate reasons as to why the claims in this group do not stand or fall together, but rather has relied on previous reasons offered with respect to other groups. Thus, examiner believes that Group VIII should be abolished and incorporated into Group IV with the resulting groups as follows:

Group I: Claims 1, 2, 5-10 and 28

Group II: Claims 40 and 42

Group III: Claims 3, 4, 29 and 30

Group IV: Claims 27, 38 and 39

Group V: Claims 11-13, 20, 33, 34, 36 and 37

Group VI: Claims 14, 21, 22 and 35

Group VII: Claims 23, 26 and 41

Group VIII: Claims 24 and 25

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

6,493,447	GOSS et al	12-2002
US 2002/0054064 A1	KANNAN	12-2001
5,784,564	CAMAISA et al	7-1998
6,181,689	CHOUNG et al	1-2001

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-2, 5-10, 28, 40 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss et al, U.S. Patent No. 6,493,447 B1 in view of Kannan, U.S. Patent Application Publication No. US 2002/0054064 A1.

As per **Claims 1, 5-10, 28, 40 and 42,** Goss et al disclose a method for effecting a synchronized browsing session between a guide terminal and a follower terminal (Abstract), the method comprising the steps of:

- providing address information corresponding to the follower terminal to the guide terminal, and from the follower terminal to the guide terminal as part of TCP/IP communications (Col. 2, lines 5-15; Col. 6, lines 50-55; Col. 7, lines 30-50);

- generating a browsing command at the guide terminal and sending the browsing command to the follower terminal (Col. 8, lines 50-63);

- receiving, with the follower terminal, the browsing command and effecting the browsing command (Col. 8, lines 50-63).

Goss et al further discloses the use of a secure web site (Col. 6, lines 30-33; Col. 12, lines 27-46), however, fails to explicitly disclose encrypting the browsing command by the guide terminal and decrypting the browsing command by the follower terminal prior to effecting the browsing command. Kannan discloses a method for providing customer service over the World Wide Web (WWW) and teaches that the customer service is provided by a secure, private, human-to-human communication between a browsing customer and a customer service representative in real-time over the web (Page 2, paragraph 0018). Kannan further teaches that secure communication can be attained because the invention incorporates a Secure Socket Layer for other Web security technique (Page 3, 0032; Page 5, 0063; Page 11, 0129) such as a Secure Hypertext Transport Protocol (Page 4, 0061), which were well known security protocols at the time of applicant's invention, designed to support various encryption and authentication measures such as public key encryption to keep all transactions secure from end to end. Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Goss et al and include the encrypting the browsing commands to provide a layer of security to the communications between the customer and the customer service representative as taught by Kannan. Kannan provides motivation by indicating that communication between a customer and a seller must also be secure and private so that the parties can ask questions and exchange personal data such as credit card information to complete the transaction (Page 1, 0010).

Goss et al further fail to specifically disclose wherein the follower terminal is configured such that at least one of downloading applets is disabled and execution of applets is disabled. Examiner, however, takes Official Notice that disabling applets is old and well known in the art and it would have been obvious to one having ordinary skill in the art to disable applets for obvious security reasons. Furthermore, applicant has admitted in the specification (page 4) that disabling applets is known.

As per **Claim 2**, Goss et al further disclose that the browsing command is a request for content associated with a URL (Col. 6, lines 2-9 and 55-65)

As per **Claim 8**, Goss et al further disclose wherein the address information corresponding to the follower terminal are provided to the guide terminal via a session manager (Figure 8, Figure 8, Col. 21, lines 8-28).

Claims 3-4, 29-30 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss et al, U.S. Patent No. 6,493,447 B1 and Kannan, U.S. Patent Application Publication No. US 2002/0054064 A1 as applied to claims 2 and 28 above, and further in view of Camaisa et al, U.S. Patent No. 5,784,564.

As per **Claims 3-4, 29-30 and 39**, the combination of Goss et al and Kannan fail to specifically disclose determining, at the follower terminal, whether or not access is permitted to the content, and if it is, then requesting the content, and if it is not permitted, then not requesting the content. Camaisa et al disclose a user terminal with a closed browser to limit or restrict access to certain content or web sites on a list and teach that if access is allowed, then requesting the content and not requesting the content when access is not permitted (Col. 2,lines 26-32 and 41-48; Col. 3, lines 19-30; Col. 4, lines 31-39; Col. 5 line 59-Col. 6 line 18). Camaisa et al teach that if access is determined to be allowed based upon a first set of rules which specify whether the content or web site is on a GO list, then the content is requested (Col. 2, lines 42-48; Col. 4, lines 15-18; Col. 5 line 59-Col. 6 line 18). Camaisa et al further disclose that if access is determined to be not allowed based upon a second set of rules which specify whether the content or web site is on a NO GO list, then the content is not requested (Col. 2,lines 26-32 and 41-48; Col. 3, lines 19-30; Col. 4, lines 31-39; Col. 5 line 59-Col. 6 line 18). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Goss et al and Kannan and include the ability to restrict access to certain content or web sites as taught by Camaisa et al. Camaisa et al provides motivation by indicating that service providers would sometimes prefer that users

be able to access the Web pages of the service providers, without affording access to other sites at their expense (Col. 1, lines 55-65), or limit access for security reasons (Col. 2, lines 1-8).

Claims 11-13, 20, 33-34 and 36-37, rejected under 35 U.S.C. 103(a) as being unpatentable over Choung et al, U.S. Patent No. 6,181,689 B1.

As per **Claims 11, 20, 33-34 and 36-37**, Choung et al disclose a method for effecting a synchronized browsing session between a guide terminal and a follower terminal (Abstract), the method comprising the steps of:

- providing address information corresponding to the follower terminal to the guide terminal, and from the follower terminal to the guide terminal (Col. 7, lines 1-13; Col. 9, lines 45-55);

- generating a browsing command at the guide terminal and sending the browsing command to the follower terminal for acceptance and in response to a request from the guide terminal (Col. 7, lines 27-35);

- receiving, with the follower terminal, the browsing command and effecting the browsing command, wherein the browser at the follower terminal is resident on the follower terminal before any connection between the follower terminal and the guide terminal (Col. 7, lines 48-58);

- establishing, in response to an input at the second terminal, a call between the customer at the follower terminal and the live agent at the guide terminal and wherein the call includes audio (telephone) and video (Web browser) communications (Col. 6, lines 1-11; Col. 7, lines 14-23).

Choung et al disclose a synchronized browsing session between a guide terminal and a follower terminal without utilizing applets, however, does not explicitly disclose disabling one of downloading or executing applets. Examiner takes Official Notice, however, that disabling applets is old and well known in the art and it would have been obvious to one having ordinary skill in the art to disable applets for obvious security reasons. Furthermore, applicant has admitted in the specification (page 4) that disabling applets is known.

Furthermore, the preamble generally does not limit the claims when it merely defines the context in which the invention operates. A preamble is generally not accorded any patentable weight where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). See also *Allen Engineering Corp. v. Bartell Industries, Inc., v. Darragh Co.*, 63 USPQ2d 1769, 1774 (Fed. Cir. 2002) and *DeGeorge V. Bernier*, 226 USPQ 758, 761 n.3 (Fed. Cir. 1985).

As per **Claim 12**, Choung et al further disclose wherein the follower browser is maintained by a session manager (Figure 2).

As per **Claim 13**, Goss et al disclose a system for establishing and effecting a synchronized browsing session comprising:

- a guide terminal including a connection process for invoking the establishment of the synchronized browsing session and a process for generating synchronized browsing commands (Figure 2 and Col. 6 line 64-Col. 7 line 13; Col. 7, lines 28-35);

- a follower terminal including a connection process for facilitating the establishment of the synchronized browsing session and a process for receiving and effecting synchronized browsing commands (Figure 2 and Col. 7, lines 40-58);

- a session manager working with the connection process of the follower terminal to establish and maintain the synchronized browsing session (Figure 2, Col. 7, lines 48-58); and

- at least one network for communicating data between the guide terminal, the follower terminal and the session manager (Figure 1).

Choung et al disclose a synchronized browsing session between a guide terminal and a follower terminal without utilizing applets, however, does not explicitly disclose that the follower terminal is configured for disabling one of downloading or executing applets. Examiner takes Official Notice, however, that disabling applets is old and well known in the art and it would have been obvious to one

having ordinary skill in the art to disable applets for obvious security reasons. Furthermore, applicant has admitted in the specification (page 4) that disabling applets is known.

Claims 14, 21-22 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Choung et al, U.S. Patent No. 6,181,689 B1 in view of Kannan, U.S. Patent Application Publication No. 2001/0054064.

As per **Claims 14, 21-22 and 35**, Choung et al fail to explicitly disclose encrypting the browsing command by the guide terminal and decrypting the browsing command by the follower terminal prior to effecting the browsing command. Kannan discloses a method for providing customer service over the World Wide Web (WWW) and teaches that the customer service is provided by a secure, private, human-to-human communication between a browsing customer and a customer service representative in real-time over the web (Page 2, paragraph 0018). Kannan further teaches that secure communication can be attained because the invention incorporates a Secure Socket Layer for other Web security technique (Page 3, 0032; Page 5, 0063; Page 11, 0129) such as a Secure Hypertext Transport Protocol (Page 4, 0061), which were well known security protocols at the time of applicant's invention, designed to support various encryption and authentication measures such as public key encryption to keep all transactions secure from end to end. Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Choung et al and include the encrypting the browsing commands to provide a layer of security to the communications between the customer and the customer service representative as taught by Kannan. Kannan provides motivation by indicating that communication between a customer and a seller must also be secure and private so that the parties can ask questions and exchange personal data such as credit card information to complete the transaction (Page 1, 0010).

Claims 23, 26-27, 38 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss et al, U.S. Patent No. 6,493,447 B1 in view of Camaisa et al, U.S. Patent No. 5,784,564

As per **Claims 23, 26-27, 38 and 41**, Goss et al disclose, in a follower terminal, a method for effecting a synchronized browsing session with a guide terminal comprising the steps of accepting and acknowledging a browsing command from the guide terminal (Col. 8, lines 50-63). Goss et al, however, fail to explicitly disclose whether access is permitted to the content, and if it is, then requesting the content. Camaisa et al disclose a user terminal with a closed browser to limit or restrict access to certain content or web sites on a list. Camaisa et al teach that if access is determined to be allowed based upon a first set of rules which specify whether the content or web site is on a GO list, then the content is requested (Col. 2, lines 42-48; Col. 4, lines 15-18; Col. 5 line 59-Col. 6 line 18). Camaisa et al further disclose that if access is determined to be not allowed based upon a second set of rules which specify whether the content or web site is on a NO GO list, then the content is not requested (Col. 2,lines 26-32 and 41-48; Col. 3, lines 19-30; Col. 4, lines 31-39; Col. 5 line 59-Col. 6 line 18). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Goss et al and Kannan and include the ability to restrict access to certain content or web sites as taught by Camaisa et al. Camaisa et al provides motivation by indicating that service providers would sometimes prefer that users be able to access the Web pages of the service providers, without affording access to other sites at their expense (Col. 1, lines 55-65), or limit access for security reasons (Col. 2, lines 1-8).

Goss et al fails to explicitly disclose that the follower terminal is configured for disabling one of downloading or executing applets. Examiner takes Official Notice, however, that disabling applets is old and well known in the art and it would have been obvious to one having ordinary skill in the art to disable applets for obvious security reasons. Furthermore, applicant has admitted in the specification (page 4) that disabling applets is known.

Claims 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss et al, U.S. Patent No. 6,493,447 B1 and Camaisa et al, U.S. Patent No. 5,784,564 as applied to claim 23 above, and further in view of Kannan, U.S. Patent Application Publication No. US 2002/0054064 A1.

As per **Claims 24-25**, Goss et al and Camaisa et al fail to explicitly disclose the encrypting the browsing command and the acknowledge reply between the guide terminal and the follower terminal. Kannan discloses a method for providing customer service over the World Wide Web (WWW) and teaches that the customer service is provided by a secure, private, human-to-human communication between a browsing customer and a customer service representative in real-time over the web (Page 2, paragraph 0018). Kannan further teaches that secure communication can be attained because the invention incorporates a Secure Socket Layer for other Web security technique (Page 3, 0032; Page 5, 0063; Page 11, 0129) such as a Secure Hypertext Transport Protocol (Page 4, 0061), which were well known security protocols at the time of applicant's invention, designed to support various encryption and authentication measures such as public key encryption to keep all transactions secure from end to end. Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Goss et al and include the encrypting the browsing commands to provide a layer of security to the communications between the customer and the customer service representative as taught by Kannan. Kannan provides motivation by indicating that communication between a customer and a seller must also be secure and private so that the parties can ask questions and exchange personal data such as credit card information to complete the transaction (Page 1, 0010).

(11) Response to Argument

Group I (Claims 1, 2, 5-10, 28, 40 and 42)

Appellant argues that the references to Goss and Kannan fail to teach or suggest encrypting a synchronized browsing command. Appellant further argues that it would not have been obvious to modify the method of Goss to encrypt browsing commands in view of the teachings of Secure Socket Layer (SSL) offered by Kannan. Appellant asserts that the security measures espoused in Kannan are apparently limited to securing personal information, such as questions, personal data, and credit card information, needed "to complete a commercial transaction". Examiner submits that Goss teaches sending a synchronized browsing command to a follower terminal, however, does not disclose that the transmission of this command is encrypted. Examiner indicated previously that encrypting data that is transmitted between two terminals or parties by using various encryption techniques in well known in the

art for obvious reasons of security. Kannan offers evidence of this by teaching a method for providing secure communications between a browsing customer and a customer service representative in real-time over the web by incorporating a well known Secure Socket Layer protocol (0032; 0061; 0063; 0129) or other Web security technique such as Secure Hypertext Transport Protocol (0032; 0061). SSL was well known at the time of applicant's invention as a security protocol designed to support various encryption and authentication measures such as public key encryption to keep all transactions secure from end to end and Kannan indicates that SSL is supported by current browsers and is a widely used protocol for implementing cryptography in the Web (0129). SSL is defined as "A protocol developed by Netscape Communications Corporation for ensuring security and privacy in Internet communications. SSL supports authentication of client, server, or both, as well as encryption during a communications session. While primary purpose of SSL is to enable secure electronic financial transactions on the World Wide Web, it is designed to work with other Internet services as well. This technology, which uses public key encryption, is incorporated into the Netscape Navigator Web browser and Netscape's commerce servers" by Microsoft Computer Dictionary, Fourth Edition, Copyright 1999. Thus, examiner submits that since Kannan teaches that the communications over a communication network such as the Internet may include the use of SSL, it would have been obvious that all messages transmitted between the customer and the customer support representative would be encrypted using public key encryption, including the browsing commands sent from a guide terminal to a follower terminal taught by Goss. Examiner further disagrees with the notion that the security measures offered by Kannan are limited to securing personal information, such as questions, personal data, and credit card information, needed "to complete a commercial transaction". Examiner respectfully submits that is but one reason or example, among many, for implementing a secure protocol such as SSL between two parties over the Internet, but does not in any way limit the teachings of Kannan to only these scenarios. Kannan specifically discloses that the invention provides secure customer service over the Web using Web-based security techniques and one preferred example includes providing security for each of the communications over links 500 and 501 through the use of a Secure Socket Layer (SSL)(0129).

Group II (Claims 40 and 42)

Appellant argues that there is no suggestion why one skilled in the art would be motivated to disabling the downloading and/or executing applets since the Goss and Kannan references rely on applets to function. Examiner submits that although Goss and Kannan use Java applets for functionality, the reference to Kannan specifically teaches that the invention is not intended to be limited to Java or Java enabled browsers, and can be implemented in any programming language and browser, developed now or in the future, as would be apparent to a person skilled in the art. Kannan indicates that after reading his description, it will become apparent to a person skilled in the relevant art how to implement the invention in alternative environments (0061, 0066). Furthermore, the use of applets is well known in the art to introduce security risks as acknowledged by the applicant (See page 4 of specification). Naturally, one skilled in the art would be interested in avoiding the downloading and/or execution of applets in environments where security is an issue. Appellant further admits that the ability to disable the download and/or execution of applets is an optional setting built in to most browser software (See page 4 of specification). Thus, examiner submits that it would have been obvious to one having ordinary skill in the art to disable the download and/or execution of applets since applicant admits that it is a well known fact that applets pose a security risk, since browser software includes the ability to disable applets as admitted by applicant, and further since Kannan provides a specific suggestion that the invention is not intended to be limited to Java applets or Java enabled browsers, and can be implemented in any programming language and browser, developed now or in the future. Furthermore, claim 40 recites "...configured such that at least one of downloading applets is disabled and execution of applets is disabled. Examiner interprets this language such that the prior art needs only to teach either disabling the download of applets or disabling the execution of applets, but not both. This claim language certainly seems to leave open the possibility of downloading an applet at any specified time such as before disabling the download of an applet using the browser optional setting, and then after the download is complete, disabling the downloading of additional applets using a browser optional setting, thereby allowing for execution of a previously downloaded applet.

Group III (Claims 3, 4, 29 and 30)

Appellant asserts that one skilled in the art would not have been motivated to combine the patent of Camaisa with the patents of Goss and Kannan. Appellant argues that restricting a user's access may be a legitimate concern in a system such as the Camaisa patent where browsing is unguided, however, this does not suggest restricting access in a system where a guide terminal leads a synchronized browsing session. Examiner submits, however, that the language of claim 3 is recited such that the determination of access is carried out at the follower terminal (such as a customers terminal) and is not related to any processing carried out at the guide terminal. Camaisa, as admitted by the appellant, teaches restricting access by the consumer's terminal to certain content or web sites. Examiner submits that just because the Camaisa patent does not disclose a synchronized browsing session similar to Goss and Kannan does not mean that the teachings or suggestions provided by Camaisa would not have been useful or obvious to one having ordinary skill in the art. The specific issue at hand in claim 3 is whether or not the follower terminal should be granted access to certain content. Examiner submits that the Camaisa reference focuses on this issue and solves a similar problem. Appellant appears to be arguing that the reference to Camaisa is non analogous art. In response, examiner submits that it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, Camaisa is reasonably pertinent to the particular problem with which the applicant was concerned – whether or not to grant access to certain content at a consumer's terminal.

Group IV (Claims 39 , 27 and 38)

Appellant argues that Camaisa merely discloses a simple list of permissible Websites and does not teach or suggest a two-step process of (1) checking a first list to filter out, and (2) if filtered out, checking a second list to allow back in. Examiner submits that claim 39, when considered in the broadest reasonable interpretation, does not appear to suggest this two step process exactly as explained by appellant. See *Springs Window Fashions LP v. Novo Industries, L.P.*, 65 USPQ2d 1826, 1830 (Fed. Cir.

2003). Claim 39 simply recites setting that status to NO GO when the browsing command includes a resource locator that has a NO GO status based on first rules and setting the status to GO when the browsing command includes a resource locator that has a GO status based on second rules. Examiner further submits that Camaisa discloses this feature in accordance with the rejection above.

Group V (Claims 11-13, 20, 33, 34, 36 and 37)

Appellant first argues that Choung neither teaches nor suggests sending, from a guide terminal to a follower terminal, a browsing command. Appellant argues that Choung teaches a guide terminal sending location information rather than a browsing command. Examiner respectfully disagrees with this characterization of the Choung reference and submits that Choung teaches, as appellant has pointed out, that the guide terminal sends location information for the new web page in the form of a Uniform Resource Locator (URL) to one or more follower terminals (Col. 7, lines 31-47). Subsequently, the web browser in the following terminal loads the new web page based on the new web page location information (Col. 7, lines 53-58). The term Uniform Resource Locator (URL) is defined as "An address for a resource on the Internet. URLs are used by Web browsers to locate Internet resources. A URL specifies the protocol to be used in accessing the resource (such as http: for a World Wide Web page or ftp: for an FTP site), the name of the server on which the resource resides (such as //www.whitehouse.gov), and, optionally, the path to a resource (such as an HTML document or a file on that server)" by Microsoft Computer Dictionary, Fourth Edition, copyright 1999. Thus, examiner interprets the URL information taught by Choung to be a browsing command since the browser specifically uses this information to carry out a procedure of loading a new web page. Furthermore, appellant's own specification indicates that the browsing commands may include GO TO URL (Specification page 44 line 32) which examiner submits is taught by Choung by sending URL information to the follower terminal.

Appellant secondly argues that Choung neither teaches nor suggests a follower terminal such that downloading applets and/or execution of applets is disabled. Examiner reiterates that this language appears only in the preamble of claim 11. Examiner submits that the preamble generally does not limit the claims when it merely defines the context in which the invention operates. A preamble is generally

not accorded any patentable weight where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). See also *Allen Engineering Corp. v. Bartell Industries, Inc., v. Darragh Co.*, 63 USPQ2d 1769, 1774 (Fed. Cir. 2002) and *DeGeorge V. Bernier,* 226 USPQ 758, 761 n.3 (Fed. Cir. 1985). In claim 11, the body of the claim does not depend on this language in the preamble for completeness and the process steps are able to stand alone. Thus, this language appearing in the preamble should not be afforded any patentable weight.

Group VI (Claims 14, 21, 22 and 35)

With regard to the claims in this group, appellant simply repeats arguments previously presented relating to encrypting a browsing command. Examiner submits that the same rationale applies in this group as that provided in Group I and need not be repeated here.

Group VII (Claims 23, 26 and 41)

With regard to the claims in this group, appellant simply repeats arguments previously presented relating to restricting access to content. Examiner submits that the same rationale applies in this group as that provided in Group III and need not be repeated here.

Group VIII (Claims 24 and 25)

With regard to the claims in this group, appellant simply repeats arguments previously presented relating to encrypting a browsing command. Examiner submits that the same rationale applies in this group as that provided in Group I and need not be repeated here.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,
John W Hayes
Primary Examiner
Art Unit 3621

March 19, 2004

Conferees

James Trammell, SPE 3621

Sam Sough, SPE 3628

LEONARD C. SUCHYTA
C/O CHRILSTEN R. ANDERSON
VERIZON SERVICES GROUP
600 HIDDEN RIDGE DRIVE MAIL CODE HQE03H01
IRVING, TX 75038